

LDAP

Basic configuration is the name of the LDAP server and domain that is binded to the application

- IdapServer
- IdapDomainDefault

All configuration options are found in: Policy#Active directory

Synchronization options

Different options for LDAP integration exists

1. Validate credentials: Check username/password against LDAP
2. Maintain groups: Add missing groups as defined in the LDAP
3. Create missing users: Create users with correct LDAP credentials

Credential validation (1) is mandatory, while group synchronization (2) and automatic user creation (3) is optional.

1. IdapAuthentication
2. IdapMaintainGroupsOnLogon
3. IdapCreateUsers

Groups and usersd in Tempus Serva will be marked with the LDAP path of the object. This path is also editable, so that groups or users can be mapped to other names in Tempus Serva than in the LDAP.

Failover mechanism

In case the LDAP is not responding the server can be allowed to use local application credentials:

- IdapAuthenticationFallback

The server will initially try to validate against the LDAP, after which the validation is done against the local user table. In order to allow this operation, an encrypted copy of the user password is stored on every successful LDAP authentication. Note this behaviour is only active if the fallback

authentication is enabled.

LDAP service account

In order to communicate with the LDAP server, the Tempus Serva application will need its own account to carry out many of the synchronization operations:

- ldapUsername
- ldapPassword

No permissions except lookup rights are required for this role.

Revision #1

Created 8 April 2025 13:28:36 by Theis Villumsen

Updated 8 April 2025 13:29:02 by Theis Villumsen